

UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION

BREANDAN COTTER and
JACK DINH, individually and
on behalf of others similarly situated,

Plaintiffs,

v.

Case No. 8:19-cv-1386-VMC-CPT

CHECKERS DRIVE-IN
RESTAURANTS, INC.,

Defendant.

_____ /

REPORT AND RECOMMENDATION

Before me on referral are the Plaintiffs' Unopposed Motion for Final Approval of Class Action Settlement (Doc. 48) and the Plaintiffs' Motion for Attorneys' Fees, Costs, Expenses, and Service Awards (Doc. 47). For the reasons discussed below, I respectfully recommend that (1) the Plaintiffs' motion for final settlement approval be denied without prejudice; (2) the Plaintiffs' request for attorneys' fees, costs, expenses, and service awards be denied without prejudice; and (3) the Plaintiffs be allowed to amend their complaint to address the issue of standing in light of the Supreme Court's and the Eleventh Circuit's recent decisions on the matter. *See TransUnion LLC v.*

Ramirez, 594 U.S. ___, 2021 WL 2599472 (U.S. June 25, 2021); *In re Equifax Inc. Customer Data Sec. Breach Litig.*, ___ F.3d ___, 2021 WL 2250845 (11th Cir. June 3, 2021); *Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332 (11th Cir. 2021); *Muransky v. Godiva Chocolatier, Inc.*, 979 F.3d 917 (11th Cir. 2020) (en banc).

I.

The background of this case was previously detailed in a prior Order of the Court (Doc. 46) but bears repeating here, with some supplementation. Defendant Checkers Drive-In Restaurants, Inc. (Defendant or Checkers) is a Delaware corporation that operates over 850 restaurants in twenty-nine states and the District of Columbia. (Doc. 40). When customers use their credit or debit cards to make purchases at a Checkers restaurant, Checkers collects payment card data (PCD) related to those cards, including the cardholders' names, their account numbers, the cards' expiration dates, and the card verification value (CVV). *Id.* Checkers stores this information in its point-of-sale system and transmits it to a third party for completion of the payment. *Id.*

Beginning in or around September 2016, hackers utilizing malicious software accessed Checkers's point-of-sale systems at its restaurants throughout the United States and stole copies of customers' PCD and other private information (collectively, personally identifying information or PII). *Id.* While the dates vary by location, the

malware in question remained on Checkers's point-of-sale devices through April 2019. *Id.*¹

In June and July 2019, Plaintiffs Breandan Cotter and Jack Dinh initiated separate class actions against Checkers in this District and in the Central District of California, respectively. *See* (Doc. 1); *Dinh v. Checkers Drive-In Rests., Inc.*, No. 8:19-cv-1310-JVS-KES, Doc. 1 (C.D. Cal. July 2, 2019). The parties thereafter agreed to consolidate the two cases into the present action, however, and—to that end—Cotter and Dinh filed an amended complaint in this District in April 2020. (Doc. 40; Doc. 48 at 2). In their revised complaint, the Plaintiffs assert claims for negligence, negligence per se, unjust enrichment, declaratory judgment, breach of implied contract, breach of confidence, as well as violations of the Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. §§ 501.201, *et seq.*, California's disposal of business records statute, Cal. Civ. Code §§ 1798.80, *et seq.*, and the California Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200, *et seq.* (Doc. 40). In support of these claims, the Plaintiffs allege, *inter alia*, that Checkers failed to ensure that access to its data networks was reasonably safeguarded, failed to acknowledge and act upon industry warnings, and failed to use proper security systems. *Id.* The Plaintiffs also

¹ For ease of reference, the parties refer to this malware attack in their submissions as the “Data Breach” or the “Data Breach Incident.” I will do the same.

allege that Checkers neglected to provide timely and adequate notice to the Plaintiffs and other class members that their PII had been stolen. *Id.*

Before Checkers answered the Plaintiffs' amended complaint, the parties—through their counsel—entered into a Settlement Agreement and Release (Settlement Agreement or Settlement) on a class-wide basis. *See* (Doc. 43-1). In a subsequent motion for preliminary approval of that settlement (Doc. 43), the Plaintiffs outlined the agreement's key terms, which include the following:²

- A Settlement Class defined as: “all residents of the United States who made a credit or debit card purchase at any [a]ffected [Checkers r]estaurant during the period of the Data Breach Incident;”
- Checkers's agreement to provide a cash payment for reimbursement of up to \$5,000 per Class member for documented out-of-pocket expenses and time spent dealing with the Data Breach or compensation in the form of four vouchers of five dollars each that may be redeemed at any Checkers restaurant, for non-documented losses and time spent dealing with the repercussions of the Data Breach;
- Checkers's agreement to take remedial, data security measures, including: (a) mandatory cybersecurity and data privacy training for all managers within its organization, including corporate-owned and franchisee-owned restaurants, over the next two years; and (b) ensuring that each corporate-owned and franchisee-owned restaurant will implement a solution that encrypts payment card data when it is read by the card acceptance device/point of sale system and routes the authorization message out to the payment card networks

² Except as otherwise indicated herein, the capitalized terms used in this Report and Recommendation have the same meaning as defined in the Settlement Agreement.

without the authorization message data being unencrypted on devices owned and managed by Checkers or its franchisees;

- An agreement to use Angeion Group, LLC, as the Settlement Administrator to provide Notice to the Class Members, establish a Settlement Website, and handle all claims and requests for exclusion that are submitted;
- Checkers's agreement to pay for all costs associated with settlement administration, including the expenses of the Settlement Administrator, as well as the costs of Claims Administration, attorneys' fees, costs, and expenses of Class Counsel, and service awards to the Representative Plaintiffs;
- The appointment of Tina Wolfson and Bradley K. King of Ahdoot & Wolfson, PC, Jean Sutton Martin of Morgan & Morgan, and Abbas Kazerounian and Jason A. Ibey, Esq. of Kazerouni Law Group, APC, as Class Counsel;
- Checkers's agreement to pay Class Counsel's attorneys' fees up to \$575,000 to be approved by the Court; and
- Payment of a court-approved service award to the Representative Plaintiffs not to exceed \$2,500.

(Docs. 43, 43-1).

The Court ultimately granted the Plaintiffs' motion for preliminary approval of the settlement and entered an Order, in which it: (1) provisionally certified the Settlement Class; (2) found that (a) the Settlement Class is so numerous that joinder of all Settlement Class Members would be impracticable; (b) there are issues of law and fact common to the Settlement Class; (c) the claims of the Representative Plaintiffs

are typical of, and arise from, the same operative facts and seek similar relief as the claims of the Settlement Class Members; (d) the Representative Plaintiffs and Settlement Class Counsel will fairly and adequately protect the interests of the Settlement Class as the Representative Plaintiffs have no interests antagonistic to, or in conflict with, the Settlement Class and have retained experienced and competent counsel to prosecute this matter on behalf of the Settlement Class; (e) questions of law or fact common to Settlement Class Members predominate over any questions affecting only individual members; and (f) a class action and class settlement is superior to other methods available for a fair and efficient resolution of this controversy; (3) provisionally designated Cotter and Dinh as the Representative Plaintiffs; (4) appointed attorneys Wolfson, King, Martin, Kazerounian, and Ibey as Class Counsel; (5) determined that the proposed Settlement is fair, reasonable, and adequate to warrant providing notice of the Settlement to the Settlement Class; (6) approved the proposed Notice Program set forth in the Settlement Agreement, as well as the Claim Form, Publication Notice, Long Notice, and E-Mail Notice attached to the Settlement Agreement; (7) directed the Settlement Administrator to carry out the Notice Program in conformance with the Settlement Agreement; (8) scheduled a final fairness hearing and set deadlines associated with that hearing; (9) ordered that any Settlement Class Member who wished to be excluded from the Settlement Class electronically submit an exclusion request on the Settlement Website, or mail a written

notification of the intent to exclude himself or herself from the Settlement Class to the Settlement Administrator at the address provided in the Notice, postmarked no later than 120 days after entry of the Court's Order; and (10) mandated that any Settlement Class Member seeking to object to the Settlement Agreement timely submit a written notice of his or her objection no later than 120 days after entry of the Court's Order. (Doc. 46).

The instant motions followed. (Docs. 47, 48). By way of those motions, the Plaintiffs request that the Court: (1) certify the Settlement Class for settlement purposes; (2) approve the Settlement Agreement; and (3) dismiss the action with prejudice. (Doc. 48). The Plaintiffs also ask that the Court approve payment of their agreed-upon service awards of \$2,500, as well as an award of attorneys' fees and expenses to Class Counsel in the amount of \$575,000. (Doc. 47).

I conducted a final fairness hearing relative to these topics, after which I directed supplemental briefing on the question of the Plaintiffs' standing to pursue their claims. (Doc. 57). The Plaintiffs submitted memoranda addressing this issue (Doc. 58), while Checkers filed a notice stating that it took no position on the matter (Doc. 59).

Soon thereafter, in February 2021, the Eleventh Circuit handed down its decision in *Tsao*, in which it applied the teachings from its *en banc* decision several months earlier in *Muransky* to resolve the issue of standing in the context of a class action complaint involving a data breach. *Tsao*, 986 F.3d at 1339. Given the

apparent relevance of *Tsao* to this case, I instructed the parties to provide further briefing on the standing question. (Doc. 60). The Plaintiffs complied with this directive and tendered supplemental declarations on the issue. (Docs. 61, 62). As before, Checkers took no position on the matter. (Doc. 63).

In early June 2021, the Eleventh Circuit decided *Equifax*, in which it confronted yet another standing challenge in the context of a data breach class action. 2021 WL 2250845, at *1. The Plaintiffs filed a Notice of Supplemental Authority offering their views on this decision the following week. (Doc. 64).

Later in June 2021, the Supreme Court filed its opinion in *TransUnion*, in which it ruled on the question of standing for members of a class asserting claims under the Fair Credit Reporting Act (FCRA). 2021 WL 2599472. With the benefit of the guidance afforded by the Supreme Court in *TransUnion* and the Eleventh Circuit in *Muransky*, *Tsao*, and *Equifax*, the Plaintiffs' motions are now ripe for the Court's resolution.

II.

Article III of the Constitution limits the power of the federal courts to deciding “cases” and “controversies.” U.S. Const. art. III, § 2. For there to be a case or controversy under Article III, a plaintiff must have standing. *TransUnion*, 2021 WL 2599472, at *6 (citation omitted); *Spokeo, Inc. v. Robins*, 578 U.S. ___, 136 S. Ct. 1540, 1547 (2016); *Muransky*, 979 F.3d at 924.

To establish standing, “a plaintiff must show (i) that he suffered an injury in fact that is concrete, particularized, and actual or imminent; (ii) that the injury was likely caused by the defendant; and (iii) that the injury would likely be redressed by judicial relief.” *TransUnion*, 2021 WL 2599472, at *6 (citing *Lujan v. Defenders of Wildlife*, 504 U. S. 555, 560–561 (1992)); *see also Spokeo*, 136 S. Ct. at 1547 (citations omitted). A plaintiff bears the burden of satisfying each of these elements. *TransUnion*, 2021 WL 2599472, at *10; *Tsao*, 986 F.3d at 1337 (citation omitted). Further, a plaintiff must demonstrate standing for each claim he asserts and for each form of relief he seeks. *TransUnion*, 2021 WL 2599472, at *10 (citations omitted).

Of the three criteria for standing, the one at issue here is injury in fact. To meet this requirement, a plaintiff must plausibly and clearly allege an injury that is “concrete” and either “actual or imminent.” *Tsao*, 986 F.3d at 1337–38 (quoting *Thole v. U.S. Bank N.A.*, 590 U.S. ___, 140 S. Ct. 1615, 1621 (2020) and *Spokeo*, 136 S. Ct. at 1548); *see also Muransky*, 979 F.3d at 925 (“A plaintiff needs to plead (and later support) an injury that is concrete, particularized, and actual or imminent, rather than conjectural or hypothetical.”) (citation omitted). The Supreme Court has defined a “concrete” injury as one that is “real, and not abstract”—that is, one that “actually exist[s];” and an “actual or imminent” injury as one that is neither “conjectural [n]or hypothetical.” *Spokeo*, 136 S. Ct. at 1548 (internal quotation marks and citation

omitted).³ Examples of concrete injuries include physical and monetary harms, as well as “various intangible harms,” such as—of relevance here—the “disclosure of private information.” *TransUnion*, 2021 WL 2599472, at *7 (citations omitted).

Where a plaintiff attempts to satisfy the injury in fact element by relying on future harm, the “threatened injury must be *certainly impending*.” *Clapper v. Amnesty Int’l USA*, 568 U.S. 398, 409 (2013) (internal quotation marks and citation omitted) (emphasis in original). Thus, “[a]llegations of *possible* future injury are not sufficient.” *Id.* (internal quotation marks and citation omitted) (emphasis in original); *see also TransUnion*, 2021 WL 2599472, at *15 (noting that “the risk of future harm on its own does not support Article III standing for [a] plaintiff[’s] damages claim”). Although this standard does not mandate a plaintiff demonstrate it is “‘literally certain that the harms [he] identif[ies] will come about,’” it does require, at the very least, “a showing that there is a ‘substantial risk’ that the harm will occur.” *Tsao*, 986 F.3d at 1338–39 (quoting *Clapper*, 568 U.S. at 414 n.5). If “the hypothetical harm alleged is not ‘certainly impending,’” or if “there is not a substantial risk of the harm, a plaintiff cannot conjure standing by inflicting some direct harm on [himself] to mitigate a

³ The Supreme Court in *TransUnion* stated that the “concrete-harm requirement” should also include an evaluation of “whether the alleged injury to the plaintiff has a ‘close relationship’ to a harm ‘traditionally’ recognized as providing a basis for a lawsuit in American courts.” *TransUnion*, 2021 WL 2599472, at *7 (quoting *Spokeo*, 578 U. S. at 341).

perceived risk.” *Id.* at 1339 (citing *Clapper*, 568 U.S. at 416; *Muransky*, 979 F.3d at 933).

In *Tsao*, the Eleventh Circuit was called upon to address the standing issue under circumstances very similar to those present here. 986 F.3d 1332. In that case, the named plaintiff—Tsao—filed a proposed class action complaint against the restaurant chain PDQ arising from a data breach that allegedly exposed personal financial information of PDQ’s customers, including the names of cardholders, their credit card numbers, the credit card expiration dates, and the CVVs. *Id.* at 1335. When Tsao learned of the possible breach, he cancelled the cards he had used to make purchases at PDQ during the relevant period. *Id.* In his complaint, Tsao averred that the cancellation of these credit cards temporarily deprived him of the opportunity to accrue rewards affiliated with the cards, forced him to expend time and effort to cancel the cards and to deal with the impact of the data breach itself, and resulted in him losing access to his “preferred accounts.” *Id.* at 1336–37. Tsao also included in his complaint some general information from the Federal Trade Commission and the Government Accountability Office (GAO) regarding the possible difficulties associated with cyberattacks and listed a few notable data breaches involving the restaurant industry. *Id.* at 1336.

In response to PDQ’s motion to dismiss his complaint for lack of standing, Tsao argued that he had suffered the requisite injury in fact for, among other reasons: (1)

“he and the class were at an elevated risk of future identity theft,” and (2) he had been harmed by his “efforts to mitigate the perceived risk of future identity theft.” *Id.* at 1336. The district court rejected these arguments, finding that Tsao’s allegations of injury were “conclusory” and “speculative at best.” *Id.* at 1337. The district court accordingly dismissed Tsao’s complaint, and the Eleventh Circuit affirmed on appeal. *Id.*

The Eleventh Circuit began its analysis by reviewing the case law governing standing, including its decision in *Muransky* issued in late 2020. *Id.* at 1337–39. In *Muransky*, customers of Godiva chocolate stores asserted claims for violations of the Fair and Accurate Credit Transactions Act (FACTA) on the grounds that the stores left them vulnerable to an increased threat of future identity theft by printing too many digits on their credit card receipts. *Id.* at 922. Notably, however, the injuries alleged were purely “statutory in nature”—that is, the harm to the plaintiffs was merely that the FACTA had been violated. *Id.* Notwithstanding this fact and despite a challenge made by an objector to the plaintiffs’ standing, the district court approved the settlement. *Id.* at 923.

On appeal, the Eleventh Circuit, sitting *en banc*, vacated the district court’s order and remanded the case with instructions to dismiss it for lack of standing. *Id.* at 936. Drawing on the Supreme Court’s opinions in *Clapper* and *Spokeo*, the Court reasoned, in pertinent part, that Muransky’s “naked” averments he and the other class members

were exposed only to an “elevated risk” of identity theft but had not actually been the victims of such misconduct were insufficient to confer standing. *Id.* at 931–33. The Court was also unpersuaded by Muransky’s alternative claim that he had suffered a direct injury in fact because he had spent time “destroying or safeguarding” his receipts in an attempt to reduce his exposure to future identity theft. *Id.* at 931.

Following its review of its decision in *Muransky*, the Eleventh Circuit in *Tsao* turned its attention to Tsao’s contention that he faced a “substantial risk of identity theft, fraud, and other harm in the future as a result of the [PDQ] data breach.” *Tsao*, 986 F.3d at 1340. Noting that it had not yet “addressed th[is] issue head-on,” the *Tsao* court looked initially to those circuit courts that had. *Id.* While observing that these courts were divided on the question, the Eleventh Circuit concluded that “[g]enerally speaking, the cases conferring standing after a data breach based on an increased risk of theft or misuse [of stolen information] included at least some allegations of actual misuse or actual access to personal data.” *Id.*

Of the circuit court opinions it considered, the *Tsao* court found the Eighth Circuit’s decision in *In re SuperValu, Inc.*, 870 F.3d 763 (8th Cir. 2017) both persuasive and akin to Tsao’s complaint. *Tsao*, 986 F.3d at 1343. As in *Tsao*, the plaintiffs in *SuperValu* alleged that hackers “may have accessed” their stolen credit card information and cited in support of their standing argument a GAO report describing the effects of data breaches (GAO Report). *Tsao*, 986 F.3d at 1342–43 (citing

SuperValu, 879 F.3d at 766, 770; U.S. Gov’t Accountability Off., GAO-07-737, *Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown* (2007), <https://www.gao.gov/assets/gao-07-737.pdf>). In examining the GAO Report, however, the Eighth Circuit found it to reveal that (1) compromised credit or debit card information—“without additional personal identifying information”—generally could not be utilized to open unauthorized accounts; and (2) most data breaches did not result in fraud on existing accounts. *Id.* at 1342–43. Based on these assessments, the Eighth Circuit concluded the plaintiffs in that action failed to demonstrate a substantial possibility that they would suffer identity theft in the future. 879 F.3d at 771–72. The Eighth Circuit stated in support of this conclusion that there was no claim the hackers had stolen social security numbers, birth dates, or driver’s license numbers, and thus—according to the GAO Report—the risk of identity theft was “little to no[ne].” *Id.* at 770.

Upon comparing the allegations in *SuperValu* to those before it, the Eleventh Circuit in *Tsao* found the two cases were much alike. *Tsao*, 986 F.3d at 1343. Similar to the Eighth Circuit in *SuperValu*, the *Tsao* court determined that the GAO Report actually demonstrated there was not a sufficient threat of identity theft, insofar as *Tsao* did not claim that social security numbers, birth dates, or other comparable information were compromised in the PDQ data breach. *Id.*

The Eleventh Circuit in *Tsao* went on to find that, even putting aside “the GAO Report and the reasoning in *SuperValu*,” Tsao still had not averred that he faced a substantial threat of harm or that such harm was certainly impending. *Id.* Citing *Muransky*, it stated that Tsao’s “threadbare” assertions of a “‘continuing’ risk of identity theft” were inadequate to establish standing. *Id.* It also found that Tsao offered only “vague [and] conclusory allegations that members of the class [had] suffered any actual misuse of their personal data,” such as “unauthorized charges.” *Id.* And, finally, it noted that because Tsao immediately canceled his credit cards, he “effectively eliminat[ed] the risk of credit card fraud in the future.” *Id.* at 1344.

The Eleventh Circuit in *Tsao* likewise deemed inadequate Tsao’s claims of “actual, present injuries” stemming from his “efforts to mitigate the risk of identity theft caused by the [PDQ] data breach.” *Id.* at 1344. The Court reiterated its reasoning in *Muransky* that a plaintiff, such as Tsao, could not “‘manufacture standing merely by inflicting harm on [himself] based on [his] fears of hypothetical future harm that is not certainly impending.’” *Id.* at 1344 (citations omitted). The court remarked in this regard that the “mitigation costs” Tsao asserted were “inextricably tied to his perception of the actual risk of identity theft following the PDQ data breach.” *Id.* at 1344–45.

In light of these findings, the Eleventh Circuit in *Tsao* concluded that “[e]vidence of a mere data breach does not, standing alone, satisfy the requirements of

Article III standing.” *Id.* at 1344. It also concluded that, although “evidence of actual misuse [of personal data] is not necessary for a plaintiff to establish standing following a data breach,” a plaintiff cannot meet his burden of plausibly pleading sufficient factual allegations to demonstrate certainly impending harm of future identity theft, or that there was a substantial threat of such harm, without “specific evidence of *some* misuse of class members’ data.” *Id.* at 1343–44. It further emphasized that a plaintiff cannot “conjure standing [] by inflicting injuries on himself to avoid an insubstantial, non-imminent risk of identity theft.” *Id.* at 1344–45.

Four months after deciding *Tsao*, the Eleventh Circuit issued its decision in *Equifax*. In that case, Equifax—a consumer reporting agency—was the victim of a data breach “involv[ing] some of the most sensitive personal information possible” belonging to almost 150 million Americans. *Equifax*, 2021 WL 2250845, at *2. This information included “all nine digits of [the] Americans’ Social Security numbers, coupled with their names, dates of birth, and addresses, among other things.” *Id.*

As a result of this data breach, ninety-six named plaintiffs “brought a host of statutory and common law claims under federal and state law,” claiming that the breach caused them to be “subject[ed] to a pervasive, substantial and imminent risk of identity theft and fraud.” *Id.* They also averred that the breach required them to spend “time, money, and effort attempting to mitigate the risk of identity theft” and that many had already been the victims of such theft. *Id.* The parties ultimately

agreed to settle the matter, and the district court approved that settlement following a fairness hearing. *Id.* at *2–4. Several objectors appealed, however, contending, *inter alia*, that the plaintiffs whose identities had not been stolen lacked standing because they had not suffered an injury in fact. *Id.* at *6.

The Eleventh Circuit rejected this argument, holding that “[g]iven the colossal amount of sensitive data stolen, including Social Security numbers, names, and dates of birth, and the unequivocal damage that can be done *with this type of data*, . . . [the p]laintiffs [have] adequately alleged that they face a ‘material’ and ‘substantial’ risk of identity theft that satisfies the concreteness and actual-or-imminent elements.” *Id.* (emphasis added) (citing *Muransky*, 979 F.3d at 927; *Clapper*, 568 U.S. at 414 n.5). The court additionally held that, based on the magnitude of the harm at issue, the “allegations of mitigation injuries made by the[p]laintiffs [were] also sufficient” to establish standing. *Id.* at *7 (citing *Muransky*, 979 F.3d at 931 (“[A]ny assertion of wasted time and effort necessarily rises or falls along with this Court’s determination of whether the risk posed . . . is itself a concrete harm.”)).

Roughly three weeks after *Equifax*, the Supreme Court handed down its opinion in *TransUnion*. In that case, a group of plaintiffs brought a class action against TransUnion—a credit reporting agency—for engaging in practices that allegedly contravened the FCRA. 2021 WL 2599472, at *3, *5. The crux of the plaintiffs’ claims centered around an “OFAC Name Screen Alert” which TransUnion included

as part of the consumer reports it compiled for third-party businesses seeking to check the creditworthiness of their patrons. *Id.* at *4. OFAC is the U.S. Treasury Department's Office of Foreign Assets Control, and maintains a list of "specially designated nationals" who threaten America's national security. *Id.* These individuals "are terrorists, drug traffickers, or other serious criminals," with whom it is generally unlawful to transact business. *Id.*

The named plaintiff in *TransUnion*, Sergio Ramirez, learned of TransUnion's inclusion of the OFAC Name Screen Alert in its consumer reports when he attempted to purchase a vehicle at a car dealership and was told that his name appeared on the OFAC list. *Id.* The next day, Ramirez requested a copy of his credit file from TransUnion. *Id.* at *5. Contrary to the FCRA's requirements, the mailing TransUnion subsequently sent Ramirez contained his credit file and a statutorily-mandated summary of rights form but did not mention the OFAC alert. *Id.* TransUnion sent Ramirez a second mailing the next day, which informed Ramirez that his name potentially matched a name on the OFAC list but did not include an additional copy of the summary of rights form. *Id.*

In his complaint, Ramirez asserted that TransUnion violated the FCRA by: (1) failing to follow reasonable procedures to ensure the accuracy of the information in his credit file; (2) neglecting to provide him with all information in his credit file upon his request; and (3) failing to provide him with a summary of his rights with each

mailing. *Id.* For relief, Ramirez requested statutory and punitive damages. *Id.* Ramirez also sought to certify a class of all people in the United States to whom TransUnion sent a similar mailing during the six-month period surrounding his unfortunate experience at the car dealership. *Id.* Although the class ultimately came to consist of 8,185 members, the parties stipulated that TransUnion provided third parties with credit reports for only 1,853 of those class members. *Id.*

Over TransUnion's objection, the district court certified the class and the case proceeded to trial. *Id.* At the conclusion of the trial, a jury rendered a verdict for the plaintiffs and awarded each class member roughly \$1,000 in statutory damages and more than \$6,000 in punitive damages. *Id.* TransUnion challenged the plaintiffs' standing on appeal, but the Ninth Circuit affirmed. *Id.* The Supreme Court granted a petition for writ of certiorari to address the issue of whether "either Article III or Rule 23 permits a damages class action where the vast majority of the class suffered no actual injury, let alone an injury anything like what the class representative suffered." *TransUnion LLC v. Ramirez*, 141 S. Ct. 972 (2020); Pet. For a Writ of Cert., *TransUnion LLC v. Ramirez*, No. 20-297, 2020 WL 5411253 (Sept. 2, 2020).

In a 5-4 decision, the Supreme Court reversed the Ninth Circuit's judgment and remanded the matter. 2021 WL 2599472, at *15. Of note here, the Court emphasized at the outset that, in the class action context, "[e]very class member must have Article III standing in order to recover individual damages," *id.* at *10, and that

“Article III does not give federal courts the power to order relief to any uninjured plaintiff, class action or not,” *id.* (quoting *Tyson Foods, Inc. v. Bouaphakeo*, 577 U.S. 442, 466 (2016) (Roberts, C.J., concurring)). The Court also emphasized that plaintiffs in a class action must “demonstrate standing for each claim that they press and for each form of relief that they seek,” whether it be for injunctive relief, damages, or some other remedy. *Id.* (citations omitted).

After applying “fundamental standing principles” to the facts before it, the Court “ha[d] no trouble concluding” that the 1,853 class members for whom TransUnion disseminated credit reports that allegedly included misleading OFAC alerts suffered a “concrete harm” relative to their “reasonable procedures” claim and thus had standing. *Id.* at *10–11. As to the remaining 6,332 class members, however, the Court found that the “mere existence” of misleading information in their credit files alone did not result in a concrete injury. *Id.* at *11.

The Court also found unpersuasive the alternative argument made by the 6,332 class members that they suffered a concrete injury for purposes of their “reasonable procedures” claim because the presence of misleading OFAC alerts in their internal credit files exposed them to a “material risk that the information would be disseminated in the future to third parties and thereby cause them harm.” *Id.* at *12.

The Court reasoned:

[T]he 6,332 plaintiffs did not demonstrate that the risk of future harm materialized—that is, that the inaccurate OFAC alerts in their internal

TransUnion credit files were ever provided to third parties or caused a denial of credit. Nor did those plaintiffs present evidence that the class members were independently harmed by their exposure to the risk itself—that is, that they suffered some other injury (such as an emotional injury) from the mere risk that their credit reports would be provided to third-party businesses.

Id. at *13.

The Court went on to find that even apart from the “fundamental problem with their argument based on the risk of future harm,” the 6,332 plaintiffs did not factually establish an adequate risk of future harm to support Article III standing. *Id.* at *14.

The Court explained:

[T]he plaintiffs did not demonstrate a sufficient likelihood that their individual credit information would be requested by third-party businesses and provided by TransUnion during the relevant time period. Nor did the plaintiffs demonstrate that there was a sufficient likelihood that TransUnion would otherwise intentionally or accidentally release their information to third parties. Because no evidence in the record establishes a serious likelihood of disclosure, we cannot simply presume a material risk of concrete harm.

Id. (internal quotation marks and citation omitted).

Lastly, the Court addressed standing in connection with the plaintiffs’ disclosure and summary of rights claims. The Court readily disposed of these allegations, finding that the plaintiffs (other than Ramirez) failed to demonstrate any harm at all. *Id.* at *15.⁴

⁴ The Court declined to decide whether Ramirez’s claims were typical of those of the class, as required by Rule 23, *TransUnion*, 2021 WL 2599472, at *16, or whether every class member must demonstrate

III.

In light of the rulings in *Muransky*, *Tsao*, *Equifax*, and *TransUnion*, I respectfully recommend that the Court deny the Plaintiffs’ motion for final settlement approval on the grounds that, at a minimum, the named Plaintiffs—Cotter and Dinh—have not met their burden of plausibly and clearly alleging the requisite injury in fact. *Frank v. Gaos*, 586 U.S. ___, 139 S. Ct. 1041, 1046 (2019) (“A court is powerless to approve a proposed class settlement if it lacks jurisdiction over the dispute, and federal courts lack jurisdiction if no named plaintiff has standing.”) (citing *Simon v. E. Ky. Welfare Rights Org.*, 426 U.S. 26, 40, n. 20 (1976)); *Muransky*, 979 F.3d at 924 (noting that a district court cannot approve a proposed class action settlement “if ‘no named plaintiff has standing’”) (quoting *Gaos*). In an effort to avoid this result, the Plaintiffs argue in their most recent filings that—in accordance with *Tsao*—they adequately aver a “substantial risk of identity theft, fraud, or other harm that is concrete and imminent, not merely hypothetical and conjectural” by showing “more than mere allegations of a data breach having occurred.” (Doc. 61 at 3, 4 n.1).⁵ This argument fails.

standing before a court certifies a class, *id.* at *10, n.4 (citing *Cordoba v. DIRECTV, LLC*, 942 F.3d 1259, 1277 (11th Cir. 2019)).

⁵ The Plaintiffs asserted prior to *Tsao* that they had demonstrated standing pursuant to *In re 21st Century Oncology Customer Data Security Breach Litigation*, 380 F. Supp. 3d 1243 (M.D. Fla. 2019), which identified three factors courts commonly analyzed in determining whether a plaintiff suffered an injury in fact resulting from a threat of future identity theft. See (Doc. 58) (citing *21st Century*, 380 F. Supp. 3d at 1251–54). I find that *Tsao* controls the standing analysis here and therefore do not separately consider standing under the *21st Century* factors. I reach a similar conclusion with respect to the Plaintiffs’ reliance on the Ninth Circuit’s decision in *In re Facebook, Inc. Internet Tracking Litigation*, 956

To begin, the Eleventh Circuit in *Tsao* found the nature of the compromised data important to its standing analysis and, in fact, predicated its finding that the PDQ data breach in that case did not create a sufficient risk of identity theft on the grounds that, among other things, the breach did not involve social security numbers, birth dates, or other such intimate information. *Tsao*, 986 F.3d at 1343 (“*Tsao* has not alleged that social security numbers, birth dates, or driver’s license numbers were compromised in the PDQ breach, and the [credit and debit] card information allegedly accessed by the PDQ hackers generally cannot be used alone to open unauthorized new accounts. . . . [I]t is [therefore] unlikely that the information allegedly stolen in the PDQ breach, standing alone, raises a substantial risk of identity theft.”) (internal quotation marks and citation omitted). The malware attack in this action similarly did not involve the theft of such highly personal information.⁶

In addition, the Plaintiffs’ averments regarding the “increased risk of identity theft” and actual misuse of their personal data are conclusory and thus do not confer standing for that reason as well. *Id.* at 1334. Indeed, the Plaintiffs’ assertions regarding misuse—including that the pilfered information was “placed in the hands of criminals” (Doc. 61 at 4) (citing Doc. 40 at ¶¶ 32, 75, 115)—closely resemble those rejected as “threadbare” in *Tsao*. Compare (Doc. 40 at ¶ 32), with *Tsao v. Captiva MVP*

F.3d 589 (9th Cir. 2020), *cert. denied*, 141 S. Ct. 1684 (2021), which I add is both factually and legally distinct from this case. See (Doc. 58 at 9; Doc. 61).

⁶ This fact also distinguishes this case from *Equifax*.

Rest. Partners, LLC, No. 8:18-cv-1606-WFJ-SPF, (Doc. 1 at ¶ 81.c).⁷ This is perhaps not surprising since one of the lawyers who represented Tsao is also counsel of record in this case.

In an effort to place themselves outside the reach of *Tsao*, the Plaintiffs argue that, in *Tsao*, PDQ merely notified its customers that their information “*may* have been accessed or acquired by a hacker,” *see Tsao*, No. 8:18-cv-1606-WFJ-SPF, (Doc. 1 at 18) (emphasis added), while here Checkers *confirmed* that class members’ data “was in fact accessed and stolen in the breach” (Doc. 61 at 4 n.1). In support of this assertion, the Plaintiffs refer to a “Mandiant investigation report” which they claim “confirm[s] the details of the breach, the affected locations, and the number of payment card transactions compromised.” (Doc. 61 at 4) (citing Doc. 43 at 4). I find this contention unpersuasive.

I note as a threshold matter that the Plaintiffs do not submit clear evidence or argument establishing what exactly Checkers purportedly “confirmed” with respect to the Data Breach. By way of example, the Plaintiffs do not explain where the “Mandiant investigation report” is located on the docket, and—from my own review—I cannot determine that it has even been filed with the Court. While the Plaintiffs nonetheless maintain that Checkers verified “that the hackers’ malware

⁷ Compare also (Doc. 40 at ¶ 75), with *Tsao*, No. 8:18-cv-1606-WFJ-SPF, (Doc. 1 at ¶ 9); compare also (Doc. 40 at ¶ 115), with *Tsao*, No. 8:18-cv-1606-WFJ-SPF, (Doc. 1 at ¶ 107).

targeted 105 Checkers locations and approximately 1.5 million PCD transactions,” it appears they rely solely on their own briefing in support of this proposition. (Doc. 61 at 4, n.1) (citing Doc. 58 at 7, n.3; Doc. 40 at ¶ 59; Doc. 48 at 3).⁸

Even accepting as true the Plaintiffs’ claim that Checkers affirmed the cyberattack was “targeted and directed at extracting specific information” (Doc. 61 at 5), that fact does not materially distinguish this case from *Tsao*. Although it is true that the Court in *Tsao* referenced that customer data “may” have been compromised or exposed, it ultimately required “specific evidence of *some* misuse” of that data to establish standing. 986 F.3d at 1333–34. In a similar vein, the Eighth Circuit in *SuperValu* differentiated between the *misuse* of data and the mere *access* to such data for purposes of the standing inquiry. 870 F.3d at 769–70 (noting that the plaintiffs adequately alleged that their credit card information was stolen by hackers as a result of the defendants’ security practices, but not that it was misused); *see also In re Brinker Data Incident Litig.*, 2021 WL 1405508, at *5 (M.D. Fla. Apr. 14, 2021) (finding *Tsao*’s “some misuse” standard was satisfied by *evidence* showing that the named plaintiffs experienced unauthorized charges on their accounts after a data breach, and that the payment card information taken in the breach was put on the dark web); *Hymes v. Earl Enters. Hldgs., Inc.*, 2021 WL 1781461, at *10 (M.D. Fla. Feb. 10, 2021) (finding

⁸ Plaintiffs’ allegations that they “suffered diminution in value of their PII in that it is now easily available to hackers on the dark web” (Doc. 40 at ¶ 108) is likewise vague and conclusory.

“substantial questions” based on *Muransky* and *Tsao* as to whether the plaintiffs had standing, where all plaintiffs alleged that their payment card numbers were put on the dark web for sale but certain plaintiffs did not claim that they incurred unauthorized charges or paid for extra credit monitoring). By contrast, the Plaintiffs here appear to assert merely that a hacker *accessed* their data and do not plausibly aver or establish “some misuse” of that information. *Tsao*, 986 F.3d at 1344.⁹

In an attempt to further distance themselves from the circumstances in *Tsao*, the Plaintiffs argue the Settlement Administrator and various class members can attest that other class members experienced unauthorized charges. (Doc. 61 at 4–5). To bolster this claim, the Plaintiffs rely on the following evidence: (1) a declaration by the Settlement Administrator that nine class members submitted claims showing “documented unreimbursed unauthorized charges on payment cards and/or other out-of-pocket expenses related to misuse” (Doc. 61-1 at 2); (2) a declaration by class member Contessa McCormick stating that she “experienced fraudulent activity on [her] payment card” after using it at Checkers and incurred fraudulent charges in excess of \$3,000 that were not reimbursed (Doc. 61-2 at 1); and (3) a declaration by class member Yolanda Jackson alleging that she experienced fraudulent activity on

⁹ This distinction arguably has even more importance following *TransUnion*, in which, as noted above, the Supreme Court rejected standing with respect to those class members whose reports TransUnion did not disseminate, in part because they did not demonstrate that the risk of future harm ever “materialized.” *TransUnion*, 2021 WL 2599472, at *13.

her payment card after making purchases at Checkers during the relevant time frame in excess of \$1,000, for which she did not receive reimbursement (Doc. 62-1). The Plaintiffs assert that these declarations substantiate their claims of a significant risk of identity theft and actual injury, as well as the meaningfulness of their efforts to mitigate the resulting injuries. (Doc. 61 at 4–6).

While I agree that this type of evidence may be sufficient in some instances to establish standing in the context of a class action, *see SuperValu*, 870 F.3d at 773, it does not do so here. This is because none of the above declarations show that either of the named Plaintiffs—Cotter or Dinh—suffered an injury arising from “some misuse” of their data. This deficiency is fatal to the Plaintiffs’ standing claim. *Frank*, 139 S. Ct. at 1046 (stating that courts do not have jurisdiction to approve proposed class action settlements if no named plaintiffs have standing); *Equifax*, 2021 WL 2250845, at *5 (noting that at least “one named plaintiff must have standing as to any particular claim in order for it to advance”) (citing *Wilding v. DNC Servs. Corp.*, 941 F.3d 1116, 1124–25 (11th Cir. 2019)); *Muransky*, 979 F.3d at 936 (“[I]n the absence of a named plaintiff with standing, neither th[e appellate court] nor the district court has jurisdiction over this case.”).

The Plaintiffs’ final contention is that, under *Equifax*, their allegations that some of them “have suffered injuries resulting from *actual* identity theft support the sufficiency of all Plaintiffs’ allegations that they face a *risk* of identity theft.” (Doc.

64) (emphasis in original) (quoting *Equifax*, 2021 WL 2250845, at *7). This argument is also unavailing. First, I do not read *Equifax* to overrule the well-established requirement that a named plaintiff must have standing. *In re Holsey*, 589 F. App'x 462, 466 (11th Cir. 2014) (“Under our Court’s prior-panel-precedent rule, a prior panel’s holding is binding on all subsequent panels unless and until it is overruled or undermined to the point of abrogation by the Supreme Court or by this court sitting *en banc*.”) (internal quotation marks and citation omitted). And, as noted above, neither of the named Plaintiffs in this action have shown they have standing.

Second, in *Equifax*, “dozens of Plaintiffs allege[d] they [] already had their identities stolen and thus suffered injuries in many different ways.” 2021 WL 2250845, at *7. That is not the situation here.

Apparently anticipating this finding, the Plaintiffs alternatively request leave to amend their complaint to substitute one or both of the named Plaintiffs with class members who can show evidence of out-of-pocket losses due to the misuse of their personal information. (Doc. 61 at 7–8, n.4). I find this request reasonable for several reasons. As an initial matter, the Court did not have the benefit of *Muransky*, *Tsao*, *Equifax*, or *TransUnion* when it preliminarily approved the settlement and, since that preliminary approval, the parties have performed substantial work.¹⁰ In addition, by

¹⁰ The Plaintiffs have not submitted a supplemental notice addressing *TransUnion*.

not responding to the Plaintiffs' opposition, Checkers has essentially conceded that it does not contest the proposed substitution and amendment.¹¹

Moreover, the Eleventh Circuit has suggested, at least in dicta, that an amendment to rectify a standing issue is appropriate even at this late stage. In *Muransky*, for example, the Eleventh Circuit vacated the district court's final approval of a class action settlement after finding the named plaintiff lacked standing. 979 F.3d at 935–36. In doing so, the majority of the court observed that, “[a]t any point in this series of events, [the named plaintiff] could have confronted the standing issue head on, or requested leave to amend his complaint.” *Id.* Similarly, one of the dissenting judges in *Muransky* commented that “Supreme Court precedent and procedural fairness dictate that [the named plaintiff] have an opportunity to amend his complaint or present facts in support of standing.” *Id.* at 957 (Jordan, J., dissenting).

Finally, allowing the Plaintiffs to amend their complaint would give them the opportunity to cure any deficiencies brought to light by the rulings in *Muransky*, *Tsao*, *Equifax*, and *TransUnion*. I note only in this regard that the court in *Brinker Data*, in

¹¹ In recommending this relief, I render no opinion as to whether Ms. Jackson, Ms. McCormick, or the other class members referenced in the Settlement Administrator's declaration can sufficiently allege standing or serve as a proper class representative. Because it is unclear who the Plaintiffs intend to substitute as a named plaintiff and what that person may allege, I recommend that the Court not undertake this inquiry until after a revised complaint is filed. In addition, although the Plaintiffs request that the Court defer ruling on the instant motions until after they amend their operative complaint (Doc. 61 at 7, n.4), I recommend that the Court dismiss the motions without prejudice because both require an analysis of the named representative's role. *See, e.g.*, (Doc. 47 at 16; Doc. 48 at 11, 12, 24).

addressing a similar data breach involving customers' personal and payment card information, recently elected to narrow the scope of the class following *Tsao* to “avoid later predominance issues regarding standing and the inclusion of uninjured individuals.” 2021 WL 1405508, at *6. The *Brinker Data* court did so by (1) excluding persons from the class unless they “had their data ‘misused’ per the . . . *Tsao* decision, either through experiencing fraudulent charges or it being posted on the dark web;” and (2) requiring class members to have “some injury in the form of out-of-pocket expenses or time spent to be a part of the class.” *Id.* (citing *Tsao*, 986 F.3d at 1344).¹² The Plaintiffs should be directed to fulsomely address these and all the other requirements of Rule 23 in connection with any renewed motion for settlement approval.

IV.


Based on the foregoing, I respectfully recommend that the Court

1. Deny *Plaintiffs’ Unopposed Motion for Final Approval of Class Action Settlement* (Doc. 48) without prejudice;
2. Deny *Plaintiffs’ Motion for Attorneys’ Fees, Costs, and Expenses and Service Awards* (Doc. 47) without prejudice; and

¹² In contrast, as noted above, the provisionally approved class definition in this case includes “all residents of the United States who made a credit or debit card purchase at any [a]ffected [Checkers r]estaurant during the period of the Data Breach Incident.” (Doc. 43).

3. Grant Plaintiffs permission to file a second amended complaint, within twenty (20) days of the Court's Order.

Respectfully submitted this 7th day of July 2021.


HONORABLE CHRISTOPHER P. TUITE
United States Magistrate Judge

NOTICE TO PARTIES

A party has fourteen (14) days from this date to file written objections to the Report and Recommendation's factual findings and legal conclusions. A party's failure to file written objections, or to move for an extension of time to do so, waives that party's right to challenge on appeal any unobjected-to factual finding(s) or legal conclusion(s) the District Judge adopts from the Report and Recommendation. *See* 11th Cir. R. 3-1; 28 U.S.C. § 636(b)(1).

Copies to:
Honorable Virginia M. Hernandez Covington
Counsel of record
Any unrepresented party